

REMARKS

Claims 1-20 remain pending in this application.

Claims 1-20 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting.

In the Final Office Action, the Examiner rejected claims 1-7, and 12-16 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,775,779 (*England*). Applicants respectfully traverse this rejection.

In the Final Office Action, claims 1-20 were provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of co-pending U.S. Patent Application Serial No. 09/999,881 filed on October 31, 2001. Although Applicants believe that the claims of the present invention call for an invention that is different from the claims of U.S. Patent Application Serial No. 10/047,188, in the interest of expediency, Applicants have included herein a Terminal Disclaimer and respectfully request that the Examiner's provisional rejection of claims 1-20 be withdrawn. However, it will be appreciated that the filing of the Terminal Disclaimer to obviate the Examiner's rejection is not an admission of the propriety of the rejection. *Quad Environmental Technologies Corp. vs. Union Sanitary District*, 946 F.2d 870, 20 USPQ2d 1392 (Fed Cir. 1991). See, e.g., MPEP §804.03.

In the Final Office Action dated November 2, 2005, the Examiner interpreted the multi-table memory access as the multi-ring input/output (I/O) space access. See page 8, paragraph 17 of the Final Office Action dated November 2, 2005. Applicants respectfully assert that this is a miss-application of the multi-ring security system of *England*. In other words the Examiner

mistakenly interpreted multi-ring security system of *England* to read upon the claims of the present invention. The security ring system of *England* merely relates to program codes that could be executed within a particular security ring region, depending of the security clearance of the code. The mere disclosure of program codes being executed within certain security rings does not read, disclose, or suggest the multi-table I/O space access called for by claims of the present invention. *England* is directed to a region of memory that is restricted from access by non-trusted codes; therefore, certain codes can operate in Ring B for example, but not in Ring A, where Ring A is more restrictive. However, this disclosure does not anticipate or make obvious the multi-table I/O space access called for by claim 1 of the present invention. *England* clearly lacks the multi-table access disclosure, among other elements, of claims of the present invention.

Further, contrary to Examiner statement in the Final Office Action, Applicants respectfully assert that the argued feature relating to the multi-table I/O access is indeed found in the claims. See, paragraph 20, page 9 of the Final Office Action dated November 7, 2005.

Additionally, Applicants acknowledge and appreciate that the rejections to claims 8-11 and 17-20 under 35 U.S.C. 103(a) have been withdrawn in light of Applicants' arguments. See, paragraph 19, page 9 of the Final Office Action dated November 3, 2005. Therefore, claims 8-11 and 17-20 are allowable.

Claim 1 calls for executing a software object, establishing a security level for the software object, and performing a multi-table access of an I/O space using the security levels and executing the function of the object. Execution of the function of the object includes accessing at least a portion of the I/O space. The Examiner cited col. 5, lines 55 – 67 of *England* to promote an anticipation argument against the multi-table I/O space access using at least one security level

and executing the function of the object, which includes accessing at least a portion of the I/O space. However, in contrast to claim 1 of the present invention, **England** merely discloses a multi-level security ring system, for example, ring A, ring B, etc, wherein ring A is more restrictive. The security ring of **England** is directed to a program code that is executed within the ring, such that data may be accessed to and from memory addresses designated as the ring region. See col. 5, lines 55-60. **England** discloses that the ring B program code can also initiate the execution of the code in Ring A under certain conditions, while still “guaranteeing the integrity” of ring A code. Therefore, a number of sub-rings may be implemented by ring B code. See col. 5, line 60-67. However, this disclosure of **England** does not anticipate or make obvious the concept of the multi-table I/O space access called for by claim 1 of the present invention. In other words, simply because **England** discloses a multi-ring security system, the elements relating to the multi-table access of the claims of the present invention are not anticipated.

Secure pages disclosed by **England** merely relate to an area of memory that can be restricted from access by non-trusted codes. However, multi-table I/O space access is not disclosed by **England**. **England** merely discloses a number of code modules in a secure memory where the module can access secure portions of the memory. **England** also discloses a security loader that oversees a number of modules that provide content. The memory manager of **England** controls the accessing of various pages of the secured memory, while the security is based upon a number of rings of security levels. However, **England** does not disclose the multi-table memory access called for by claims of the present invention.

England discloses an access control table 320 that provides for reading and writing to and from memory. See col. 6, lines 33-38. The access control table 320 provides for certain

address segments that may be accessed when they relate to various memory pages that may be accessed by certain programs and certain security rings. Each of the access table entries may contain data relating to access rights for a particular program combination. *See* col. 5, lines 38-40. **England** discloses that typically, one bit of each entry contains program contents wherein the contents have read privileges for the specified page. However, **England** fails to disclose a multi-table access of I/O space, as called for by claim 1 of the present invention. **England** merely discloses an access control table that is used to provide for the access of memory by program quotes.

Further, the Examiner cited col. 9, lines 42-50 and col. 10, lines 66-20 to read upon the security level for a particular software object called for by claim 1 of the present invention. However, the security level cited in these passages only relate to providing secure storage of data to each application. In other words, certain selected applications can store a decryption key using the storage facility. *See* col. 9, lines 42-47. However, **England** does not disclose or suggest establishing a security level for a software object to perform a multi-table access of I/O space.

The security manager of **England** provides a function for controlling and protecting resources for a particular secure module that has yet to run. *See* col. 10, lines 6-7. However, these passages are generally directed to the securing of certain memory locations that may be accessed by particular trusted applications. Therefore, these are also elements of the claims that are not taught, disclosed or suggested by **England**. **England** does not disclose the multi-table access provided for by the claims of the present invention. In contrast to **England**, claim 1 of the present invention calls for establishing a security level for the software object for performing a multi-table access of I/O space.

Further, claim 1 calls for performing the multi-table I/O space access using the security levels, which is not taught, disclosed, or suggested by *England*. Claim 1 (as amended) of the present invention provides for establishing a security level for the software object, using a multi-table I/O space access using the security levels, and executing the function of the object. *England* simply does not disclose various elements of claim 1, such as establishing the security level for the software object; nor does *England* disclose performing the multi-table I/O space access using one of the security levels and then executing the object. For at least the reasons mentioned above, various elements of claim 1 of the present invention are not disclosed, taught, or suggested by *England*. *England* is generally related to accessing memory by existing software modules. Claim 1 of the present invention, in contrast, is related to establishing security levels for the software object and then performing a multi-table I/O space access based upon the security level to execute the function of the object, which are elements of the claims that are not taught, disclosed, or suggest by *England*. Therefore, *England* does not teach, disclose, or suggest all of the elements of claim 1 of the present invention. Accordingly, claim 1 of the present invention is allowable.

Additionally, claims 12, 13, and 17 call for various apparatus and systems to perform the multi-table access which are not taught, disclosed, or suggested by *England* for at least the reasons cited herein.

Independent claims 1, 12, and 13 are allowable for at least the reasons cited above. Additionally, dependent claims 2-7 and 14-16, which respectively depend from claims 1 and 13, are also allowable for at least the reasons cited above.

Applicants acknowledge that the Examiner indicated that the rejections of claims 8-11 and 17-20 have been withdrawn. Therefore, claims 8-11 and 17-20 are believed to be allowable. However, in light of at least the arguments presented herein, all claims of the present invention are allowable.

Reconsideration of the present application is respectfully requested. In light of the arguments presented above, Applicants respectfully assert that claims 1-20 are allowable. In light of the arguments presented above, a Notice of Allowance is respectfully solicited.

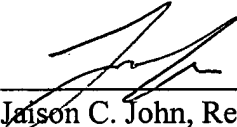
If for any reason the Examiner finds the application other than in condition for allowance, **the Examiner is requested to call the undersigned attorney at the Houston, Texas telephone number (713) 934-4069** to discuss the steps necessary for placing the application in condition for allowance.

Respectfully submitted,

WILLIAMS, MORGAN & AMERSON, P.C.
CUSTOMER NO. 23720

Date: 1/3/05

By: _____


Jason C. John, Reg. No. 50,737
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-7000
(713) 934-7011 (facsimile)
ATTORNEY FOR APPLICANT(S)